

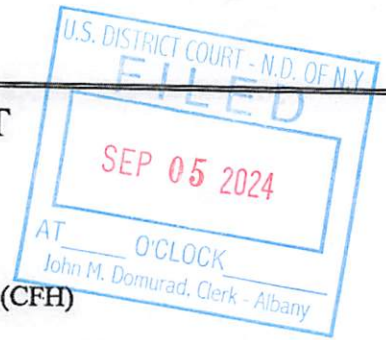
UNITED STATES DISTRICT COURT

for the
Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by
name and address)

ONE BLUE SAMSUNG CELLULAR PHONE WITH
IMEI 350256483508366, CURRENTLY LOCATED
AT A SECURE FBI FACILITY IN SARATOGA
COUNTY, NEW YORK

Case No. 1:24-mj-377-2 (CFH)



APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 2252A(a)(2)

18 U.S.C. § 2252A(a)(5)

Offense Description

Receipt of Child Pornography

Access With Intent to View/Possession of Child
Pornography

The application is based on these facts:

See attached affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

TFO Christopher Smith
Applicant's signature

TFO Christopher Smith, FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone (specify reliable electronic means).

Date: September 5, 2024

City and state: Albany, New York

Christian F. Hummel
Judge's signature

Hon. Christian F. Hummel, U.S. Magistrate Judge
Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK**

**IN THE MATTER OF THE SEARCH OF
ONE BLUE SAMSUNG CELLULAR PHONE
WITH IMEI 350256483508366, CURRENTLY
LOCATED AT A SECURE FBI FACILITY IN
SARATOGA COUNTY, NEW YORK**

Case No. 1:24-mj-377-2 (CFH)

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Christopher Smith, having been duly sworn, do hereby depose and state as follows:

1. I am an investigator with the Colonie Police Department and Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI). I have been employed by the Colonie Police Department since July 2004 and a TFO with the FBI since 2012. I am assigned full-time to the Albany Division, Albany, N.Y. I have investigated a variety of violent crimes including child sexual exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A. I have received training in the area of child sexual exploitation and have observed and reviewed numerous examples of child pornography in all forms of media including computer media. My investigative experience includes interviewing victims and witnesses, as well as conducting searches of physical locations, social media, and electronic devices pursuant to court order or consent.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device: one blue Samsung cellular phone with IMEI 350256483508366 (“SUBJECT DEVICE” or “Device”) —currently located in law enforcement possession (located at a secure FBI facility

in Saratoga County, New York), and the extraction from that property of electronically stored information described in Attachment B.

3. The facts in this affidavit come from my training and experience, information provided by members of the FBI's Child Exploitation Task Force, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that a violation of Title 18, United States Code, Sections 2252A(a)(2) (receipt of child pornography) and 2252A(a)(5) (access with intent to view and possession of child pornography) ("TARGET OFFENSES"), has been committed by EDUARDO ABREU ("ABREU") and there is probable cause to search the SUBJECT DEVICE as described below and in Attachment A for fruits and evidence of these crimes, as specifically described in Attachment B.

5. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On July 6, 2024, a police report was filed with the Colonie Police Department that ABREU commented to a 12-year-old girl, "You need a license or permit to carry around that booty." As a result, your affiant interviewed ABREU at his residence and received consent to search his Apple iPhone ("iPhone").

7. Through the course of this investigation, it was determined that ABREU was registered as a sex offender following a federal arrest in 2014. Records obtained regarding ABREU's prior arrest indicate that he was arrested following a 2013-2014 online investigation by Homeland Security Investigations (HSI). It was determined that between August 2013 and January 2014, ABREU utilized a Yahoo email to send and/or receive approximately 500 email messages that contained child pornography or links to online file sharing websites offering child pornography. In June 2014, ABREU was arrested, and a federal search warrant was executed at ABREU'S residence in Arlington, Virginia. During the execution of that search warrant, multiple electronic devices were located and forensically examined. Digital evidence containing child pornography was located on multiple electronic devices removed from ABREU'S residence that included a laptop computer and multiple external hard drives or mobile storage devices. On or around May 11, 2015, ABREU was convicted of one count of Possession of Child Pornography in violation of 18 USC 2252(a)(5)(B) and is currently a registered sex offender in the State of New York.

8. On July 8, 2024, ABREU'S iPhone was turned over the New York State Police Computer Crimes Unit ("NYSP CCU") for forensic examination. His iPhone was analyzed and the results of the examination provided to me. Contained within the forensic analysis of ABREU'S iPhone were thirty APP 1 messages that appeared to have been deleted and in the trash. APP 1 account 6536601403 "DW" was listed as owner on ABREU's iPhone and is the account associated with that cellular device. On June 11, 2024, APP 1 user 2231605040 "Cutemariana" messaged ABREU'S "DW" APP 1 account. Contained within that message were 148 attachments each containing a hyperlink and a file name, many of which are associated with child pornography, including the following:

- Blonde 11 yo BJ <https://cuty.io/xNBuvaS>
- Good sex father & daughter <https://cuty.io/f0rmPjj2lewB>
- Little schoolgirl masturbates <https://cuty.io/i1BW>
- Loliporn sexy young girl masturbate <https://cuty.io/7mNz6x8h8Q7F>
- Loliporn studio COVID-19 is a bummer! Our horny Schoolgirl <https://cuty.io/FVq957a>
- Rape daughter <https://cuty.io/7286gmUg27>
- Good sex father & daughter <https://ouo.io/rL62fEJ>
- Group sex little girls 1 <https://ouo.io/keAHlnd>
- Young girl vaginal & anal masturb <https://ouo.io/kDpgg8>
- The baby sucked a big dick and fucked <https://ouo.io/kseqmGV>
- Brunette sucked big dick <https://ouo.io/vTf9PLQ>
- Father and daughter anal sex <https://ouo.io/IM6Kr4> 1685
- Father pisses on daughter's pussy <https://ouo.io/5Rbe2Gd>
- Fucked a young girl and cum on pussy <https://ouo.io/QqkbbR>

9. On May 23, 2024, APP 1 user 2223206477 "Cutemariana" messaged ABREU'S "DW" APP 1 account. Contained within that message were 148 attachments each containing a hyperlink and a file name, many of which are associated with child sexual abuse material, including the following:

- Little schoolgirl masturbates <https://cuty.io/i1BW>
- Big penis fuck little anus <https://ouo.io/D5rJ5q>
- Chubby daughter sleeps with pink pussy 1695 <https://ouo.io/MNvg46C>
- Father fucked daughter in 69 position <https://ouo.io/1NmgsYk>
- Father licked his daughter and came on her face <https://ouo.io/nV5GUe>
- Gymnast girl anal sex <https://ouo.io/KMhM57>
- Ukrainian family daughter & mother suck dick <https://ouo.io/eNQRr1>
- Baby masturbates a small hole <https://ouo.io/GqpOfk>

10. On April 9, 2024, APP 1 user 1516157034 "Cutemariana" messaged ABREU'S "DW" APP 1 account. Contained within that message were 133 attachments each containing a hyperlink and a file name, many of which are associated with child sexual abuse material, including the following:

- Rape daughter vagina <https://cuty.io/5gGQB8RWoZ>
- Entrance with little girls. Mix <https://cuty.io/mdKhmKymdvM> Gwenet sex mother <https://cuty.io/gwFY5VVmGr>
- Older sister gives cunnilingus to little girl <https://ouo.io/xwfvJD>
- Russian girl masturbates her clitoris <https://ouo.io/IHS1ZbJ>

- Ukrainian family daughter & mother suck dick <https://ouo.io/eNQRr1>
- Baby posing for the camera <https://ouo.io/jM0eIf>
- Big dick in a small anus <https://ouo.io/AI6yyM>
- Daughter peed on mom's tits <https://ouo.io/tgGWi0>
- Family nudism <https://ouo.io/pWIFnJ>

11. Based on my training and experience, I know that many files containing child sexual abuse material are named descriptions of the image of video the file depicts.

12. Located within the forensic examination report of ABREU's iPhone was a "searched items" portion. 1,629 results were listed, many of which are indicative of a sexual interest in children. The searches were completed with the Chrome browser, including the following:

- 6/19/2024 9:07:20 PM(UTC+0) Chrome Albany tween events near me.
- 6/19/2024 9:05:28 PM(UTC+0) Chrome albania ny teen events this week
- 6/19/2024 9:01:14 PM(UTC+0) Chrome teen fridays, albania public library - north albania branch, 28 jun
- 6/19/2024 8:50:41 PM(UTC+0) Chrome wild ways teen program, 16 sep
- 6/19/2024 8:43:31 PM(UTC+0) Chrome glow up party! (ages 5- 11), 9 aug
- 6/19/2024 8:34:16 PM(UTC+0) Chrome kids dance events, albania ny
- 6/19/2024 8:34:02 PM(UTC+0) Chrome albania events girls.ballet
- 6/19/2024 8:23:05 PM(UTC+0) Chrome elementary school events colonie ny 2024
- 6/18/2024 9:25:51 PM(UTC+0) Chrome tor over vpn
- 6/17/2024 7:25:55 PM(UTC+0) Chrome how to get onto dark.web for dummies
- 6/17/2024 12:11:22 AM(UTC+0) Chrome girls' lingerie for teens, crotchless
- 6/17/2024 12:11:13 AM(UTC+0) Chrome girls' lingerie for teens
- 6/16/2024 8:31:19 PM(UTC+0) Chrome what age is elementary school

13. On August 21, 2024, Your Honor signed a federal search warrant permitting the search of ABREU's residence, person, vehicle, and electronic devices and it was executed at ABREU's Latham, New York residence. See 1:24-mj-377 (CFH). The facts contained in that search warrant and supporting affidavit are incorporated by reference. During that search, a number of electronic devices were recovered, including a Lenovo laptop computer ("laptop"). The laptop and other electronic devices were sent to NYSP CCU for forensic analysis. Upon forensic

analysis of the laptop, approximately 225 images of child pornography were found. The images were located within the thumb or cache files. For example:

- a. File name 1008ffd8e9fc1c32004187a depicted a prepubescent female approximately seven or eight years old who was naked from the waist down. The child was on her back with her legs spread exposing her genitals. A pink object was inserted in the child's vagina.
- b. 12e4097a092548f7004187a depicts a prepubescent female approximately three or four years old completely naked standing in a tub with a naked adult female. The child's fingers are inside the adult female's vagina.
- c. 13020ed0ed0fff9 depicts a prepubescent female approximately five or six years old with her head on a naked adult male's stomach. The child is holding the male's penis.
- d. 1642c11f1f336df5004187a depicts a prepubescent female approximately five or six years old on her back with her legs up and spread apart. The child is spreading her labia and has a white object inserted into her anus. A second prepubescent female approximately four to six years old is performing oral sex on the first female.

14. During the August 21 execution of the search warrant at ABREU's residence, ABREU waived his *Miranda* rights and agreed to speak with your affiant and other law enforcement officers. During the interview, ABREU stated, in sum and substance, that he would access child pornography by searching for it on the TOR browser on the internet and would masturbate to images of girls between the ages of 10 and 14 years old. ABREU admitted that after accessing the child pornography using the TOR internet browser, he would download the images

to his laptop computer and then transfer the child pornography to a thumb drive. When asked where the thumb drive containing child pornography was located, ABREU stated that earlier that day, after receiving a voice message from Colonie Police Department, he had thrown the thumb drive out the passenger side window while he was driving southbound on Interstate 87 across the Twin Bridges (Thaddeus Kosciusko Bridge).

15. On August 26, 2024, Your Honor signed a sealed criminal complaint and arrest warrant charging ABREU with one count of receipt of child pornography, in violation of Title 18, United States Code section 2252A(a)(2). *See United States v. Eduardo Abreu*, 1:24-mj395 (CFH) at Dkt. 1. The facts contained in the affidavit in support of the criminal complaint are incorporated by reference. Shortly after the arrest warrant was issued, it was entered into a law enforcement database.

16. On or about the early morning of August 27, 2024, in DeWitt, New York in the Northern District of New York, local law enforcement officers observed a vehicle registered to ABREU fail to come to a complete stop at a stop sign. The DMV check showed that ABREU was a sex offender and also had an active arrest warrant, specifically the August 26, 2024 warrant signed by Your Honor. After exiting his vehicle at a motel, local police yelled at ABREU to stop after he was observed apparently unsuccessfully attempting to enter the motel. Instead of complying, defendant began to run and was eventually placed under arrest after resisting arrest. ABREAU was charged in DeWitt Town Court with Obstructing Governmental Administration in the Second Degree, Resisting Arrest, and Criminal Possession of a Controlled Substance in the Seventh Degree. The SUBJECT DEVICE was seized during a search incident to ABREU's arrest by DeWitt police. After being transported to the DeWitt Police Department, the FBI took custody

of ABREU and his property shortly thereafter on the morning of August 27, including the SUBJECT DEVICE.

17. On the afternoon of August 27, 2024, ABREU had an initial appearance before Your Honor and the complaint was unsealed. After an August 29 detention hearing, Your Honor ordered ABREU detained without bail pending trial. *See United States v. Eduardo Abreu* at Dkt. 9.

18. The SUBJECT DEVICE is currently in the lawful possession of the FBI, specifically at a secure FBI facility in Saratoga County, New York. As detailed above, it came into the FBI's possession after it was seized incident to ABREU's arrest in DeWitt, New York. Therefore, while the FBI might already have all necessary authority to examine the SUBJECT DEVICE, I seek this additional warrant out of an abundance of caution to be certain that an examination of the SUBJECT DEVICE will comply with the Fourth Amendment and other applicable laws.

19. The SUBJECT DEVICE is currently in storage at a secure FBI facility in Saratoga County, New York. In my training and experience, and from speaking with other law enforcement personnel, I know that the SUBJECT DEVICE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICE was seized by the Dewitt Police Department and first came into the possession of the FBI.

CHARACTERISTICS OF CHILD PORNOGRAPHY COLLECTORS

20. I respectfully submit that the information set forth in this affidavit establishes probable cause to believe that an individual using the SUBJECT DEVICE has committed the TARGET OFFENSES. Based on training, experience, and numerous interviews of subjects who

admitted to having a sexual interest in children, I am aware that the following characteristics are common to individuals involved in child pornography offenses:

- a. Individuals who receive and/or possess child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity, sexually suggestive poses, or from literature describing such activity.
- b. Individuals who receive and/or possess child pornography may collect sexually explicit or sexually suggestive material depicting children, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. These individuals often maintain this material for sexual arousal and gratification. Furthermore, they may use this material to lower the inhibitions of children they are attempting to seduce, to arouse a child partner, or to demonstrate the desired sexual acts.
- c. Individuals who receive and/or possess child pornography often possess and maintain copies of child pornographic material, including but not limited to pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, and tape recordings, in the privacy and security of their home. Prior investigations into these offenses have shown that child pornography offenders typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

- d. Individuals who receive and/or possess child pornography often begin their child pornography collections by obtaining child abuse material through various free avenues afforded by the Internet, like P2P file sharing. Thereafter, these individuals may escalate their activities by producing and/or distributing child pornography, for the purpose of trading this material to add to their own child pornography collection.
- e. Individuals who receive and/or possess child pornography often maintain their digital or electronic collections in a safe, secure and private environment, such as a cellular phone, computer, or surrounding area. These collections are often maintained for several years and are maintained at the individual's residence or place of employment, to afford immediate access to view the material. These collections are often maintained for several years and are kept close by, usually at the individual's residence or sometimes vehicle, to enable the collector to view the collection, which is valued highly.
- f. Individuals who receive and/or possess child pornography may correspond with others to share information and material, and rarely destroy this correspondence. These individuals often maintain lists of names, email addresses and telephone numbers of others with whom they have been in contact regarding their shared interests in child pornography

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meaning:

- a. **Wireless telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.
- b. **Digital camera:** A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for

viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. **Portable media player:** A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna

receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. **PDA:** A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. **Tablet:** A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing

the Web, sending and receiving e-mail, and participating in Internet social networks.

- g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

22. Based on my training, experience, and research, I know that the SUBJECT DEVICE has capabilities to allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on a device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIS ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of

operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to

draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

BIOMETRIC UNLOCK

27. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.
- d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- e. As discussed in this affidavit, the SUBJECT DEVICE was recovered from ABREU during a search incident to arrest. The passcode or password that would unlock the device subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device, making the use of

biometric features necessary to the execution of the search authorized by this warrant.

- f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.
- g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all.

h. Due to the foregoing, if the SUBJECT DEVICE may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who was found in possession of the SUBJECT DEVICE and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

28. This search warrant will be executed by your affiant and other FBI Special Agents, however, law enforcement officers from other agencies may be utilized by the FBI in the execution of this search warrant, to include the forensic examination of the SUBJECT DEVICES, which may analyzed at a either an FBI or other law enforcement agency computer forensic laboratory.

//

//

//

//

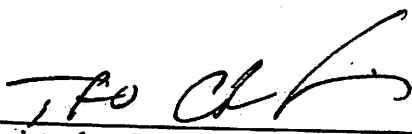
//

//

//

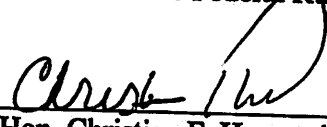
CONCLUSION

29. Based upon the above information, I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the SUBJECT DEVICE listed in Attachment A to see the items described in Attachment B.



Christopher Smith
Task Force Officer
Federal Bureau of Investigation

I, the Honorable Christian F. Hummel, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on September 5, 2024 in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.



Hon. Christian F. Hummel
United States Magistrate Judge

ATTACHMENT A

The property to be searched is one blue Samsung cellular phone, IMEI number 350256483508366, hereinafter the "SUBJECT DEVICE." The SUBJECT DEVICE is currently located at a secure FBI facility in Saratoga County, New York.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the SUBJECT DEVICE described in Attachment A that relate to violations of Title 18, United States Code, Sections 2252A(a)(2) (receipt of child pornography) and 2252A(a)(5) (access with intent to view and possession of child pornography) ("TARGET OFFENSES") and involve EDUARDO ABREU, including:
 - a. Wireless telephone or storage media used as a means to commit the violation described above;
 - b. For any wireless telephone or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "wireless telephone");
 - c. evidence of who used, owned, or controlled the wireless telephone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, text messages, photographs, and correspondence;
 - d. evidence of software that would allow others to control the wireless telephone, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - e. evidence of the lack of such malicious software;

- f. evidence indicating how and when the wireless telephone was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the wireless telephone user;
- g. evidence indicating the wireless telephone user's knowledge and/or intent as it relates to the crime(s) under investigation;
- h. evidence of the attachment to the wireless telephone of other storage devices or similar containers for electronic evidence;
- i. evidence of programs (and associated data) that are designed to eliminate data from the wireless telephone;
- j. evidence of the times the wireless telephone was used;
- k. passwords, encryption keys, and other access devices that may be necessary to access the wireless telephone;
- l. documentation and manuals that may be necessary to access the wireless telephone or to conduct a forensic examination of the wireless telephone;
- m. records of or information about Internet Protocol addresses used by the wireless telephone;
- n. records of or information about the wireless telephone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- o. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as

logs, phonebooks, saved usernames and passwords, documents, and browsing history;

- p. contextual information necessary to understand the evidence described in this attachment.
- q. records of Internet Protocol addresses used;
- r. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- s. Any and all child pornography, and any and all visual depictions of minors, including, but not limited to, sexually explicit images of minors, as those terms are defined in Title 18, United States Code, Section 2256;
- t. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2);
- u. Any and all notebooks and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2);
- v. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, and notes;
- w. Records, information, and items relating to violations of the statutes described above including:

- i. Records, information, and items relating to the occupancy or ownership of the wireless telephone;
- ii. Records, information, and items relating to the ownership or use of the wireless telephone;
- iii. Records and information relating to the identity or location of the person suspected of violating the statutes described above;
- iv. Records and information relating to sexual enticement of children, including correspondence and communications.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile/cellular phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of SUBJECT DEVICE described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual reasonably believed by law enforcement to be a user of the SUBJECT DEVICE, to the fingerprint scanner of the SUBJECT DEVICE; (2) hold the SUBJECT DEVICE in front of the face of that same individual(s) and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant